Available online at www.sciencedirect.com

SCIENCE DIRECT®

LINEAR ALGEBRA AND ITS APPLICATIONS

Linear Algebra and its Applications 378 (2004) 31–59

www.elsevier.com/locate/laa

Minimal and systematic convolutional codes over finite Abelian groups

Fabio Fagnani [a], Sandro Zampieri [b,*]

[a] *Dipartimento di Matematica, Politecnico di Torino, C.so Duca degli Abruzzi, 24, 10129 Torino, Italy*

[b] *Dipartimento di Ingegneria dell'Informazione, Università di Padova, via Gradenigo 6/a, 35131 Padova, Italy*

Received 30 January 2003; accepted 2 September 2003

Submitted by R.A. Brualdi

Abstract

Convolutional codes over Abelian groups provide an effective theoretical framework for the analysis of some classes of TCM codes. The encoder synthesis for this class of codes is not as simple as in the binary case, since minimal encoders in the group case might be necessarily nonlinear. In this contribution an algorithmic method testing whether a convolutional code over an Abelian group admits a systematic or a minimal homomorphic encoder is provided. This test consists in verifying whether a subgroup splits in a group. Through this method, the class of codes admitting systematic encoders and the class of codes admitting minimal encoders can be compared. Finally this test is applied to some examples of practical relevance.

AMS classification: 94B10; 05E15; 93B20; 93B25

Keywords: Convolutional codes; Group codes; Systems over rings; Minimal realization; Systematic encoder; Minimal encoder

1. Introduction

As shown in [10], codes with an underlying group structure play an important role in the representation of the trellis coded modulation (TCM) schemes proposed by Ungerbock in [22]. In particular, codes over Abelian groups showed to be an

* Corresponding author. Tel.: +39-049-827-7648; fax: +39-049-827-7699.
E-mail addresses: fagnani@calvino.polito.it (F. Fagnani), zampi@dei.unipd.it (S. Zampieri).

0024-3795/$ - see front matter
doi:10.1016/j.laa.2003.09.001

effective theoretical framework for the analysis of PSK modulation codes [18]. For convolutional codes over the binary field, the encoder construction is traditionally based on the theory of polynomial and rational matrices. This theory has been used for convolutional codes over Abelian groups in [18,19], where it was first pointed out that not every convolutional code admits a homomorphic systematic encoder in this set up. In general, codes over groups impose restrictions on the structural properties of the encoders they admit. While papers like [8,18,19,15] are more oriented to a clear specification of these restrictions, in [11,17] a construction of a canonical nonhomomorphic feedback free encoder is proposed.

This paper is devoted to the investigation of convolutional codes over Abelian groups which admit homomorphic encoders with special properties. It is clear that, whenever we impose restrictions on the class of codes under consideration, it is likely that the codes with the best performances are discarded. On the other hand, such a restriction allows to deal with codes in a simpler way and to select more easily the best codes in this restricted class. This is what actually happens when we consider the restriction to linear binary codes or to group codes. The same underlying philosophy motivates our interest in investigating classes of group codes admitting encoders with special structure. Moreover, there are two specific situations in which the restriction to homomorphic encoders provides great advantages. The first one is in the context of bit geometrically uniform (BGU) encoders [12], where homomorphic encoders allow a simplified computation of their bit error probability. This simplification has been successfully used for extending some results on serially concatenated turbo codes from the binary case [1] to the TCM case [12]. The second situation occurs when considering rotational invariance and rotational transparency, which can be addressed in a simpler way using homomorphic encoders [3,19].

More specifically, in this paper, as in [8], we try to characterize convolutional codes over Abelian groups which admit systematic or minimal homomorphic encoders. These codes are called systematic and minimal, respectively. Differently from [8], in this paper we do not impose restrictions on the input spaces. As a preliminary step we study the class of rational and polynomial encoders and of their inverters. In particular we show that the classical characterizations in terms of inverters of noncatastrophic and of minimal encoders continue to hold in our framework. In the second part of the paper we focus on convolutional codes. We first introduce the concept of encoding group which constitutes the input sequence space of every homomorphic encoder of the code. In general, this group does not coincide with the canonical input group of the code [11]. The first important contribution of this paper is to show that these two groups coincide exactly for the codes which admit a causal homomorphic encoder with a causal homomorphic inverse. In the free case, considered in [8], this class of codes coincides with the class of systematic and minimal convolutional codes. However, in the more general case considered in this paper, these three classes do not coincide. Systematic and minimal codes are finally characterized in purely algebraic terms precisely through the splitting property of a certain group inside another one. Moreover, these characterizations allows us to compare

minimality and systematicity. It is easily proven that a systematic convolutional code is always minimal. We show conversely that a certain power of a minimal convolutional code is necessarily systematic. In the last part of the paper these techniques are applied to some examples chosen from the codes proposed in [2]. These examples show in particular that the above mentioned classes of codes are strictly included into each other.

We conclude this section by providing a short outline of the paper. The next section is devoted to the exposition of some preliminaries on group theory and on group codes. In particular the concepts of controllability, completeness, input group and state group are recalled. Moreover, some results on operators over Laurent sequence spaces are presented. In Section 3 encoders and inverters are treated. In particular noncatastrophic, minimal and systematic encoders are investigated. In Section 4 codes are considered according to the encoders they admits and these codes are characterized in terms of group splitting. Finally Section 5 is devoted to some examples.

2. Preliminaries

In this section we will recall some preliminary definitions and results which are needed in the sequel. The first part is devoted to group theory and more specifically to splitting subgroups. In the second part some introductory material on group codes over Laurent spaces is presented, while the last part is devoted to shift operators.

2.1. Splitting subgroups

If G is any Abelian group and $n \in \mathbb{Z}$, we define the following subgroups of G:

$$G_{(n)} := \{x \in G \text{ such that } nx = 0\}, \quad nG := \{nx : x \in G\}.$$

An *exact sequence* of Abelian groups consists of a sequence of Abelian groups G_k and homomorphisms j_k as below

$$G_1 \stackrel{j_1}{\to} G_2 \stackrel{j_2}{\to} \cdots \stackrel{j_{n-1}}{\to} G_n$$

such that $\ker j_k = \operatorname{im} j_{k-1}$ for all $k = 2, \ldots, n-1$. The following exact sequence

$$\{0\} \to H \stackrel{j}{\to} G \stackrel{\pi}{\to} K \to \{0\} \tag{1}$$

is particularly important and it is called a *short exact sequence*. Notice that in this case exactness amounts to require that j is one-to-one, π is onto, and that $\ker \pi = \operatorname{im} j$. The exact sequence (1) is said to *split* if one of the two following equivalent conditions is satisfied

(i) There exists a homomorphism $\theta : G \to H$ such that $\theta \circ j = \mathrm{id}_H$.
(ii) There exists a homomorphism $p : K \to G$ such that $\pi \circ p = \mathrm{id}_K$.

The homomorphisms θ and p are called *splitting maps*. If (1) splits, then we have a natural isomorphism between G and $H \times K$ given by $g \mapsto (\theta(g), \pi(g))$.

Let H be a subgroup of G, and assume that $j : H \to G$ is the canonical injection and that $\pi : G \to G/H$ is the canonical quotient homomorphism. We say that H splits in G if the exact sequence

$$\{0\} \to H \xrightarrow{j} G \xrightarrow{\pi} G/H \to \{0\}, \tag{2}$$

splits. It can be shown that H splits in G if and only if there exists a subgroup L of G such that $G = H \oplus L$.

The following lemma provides a useful tool for checking whether a subgroup H splits in G.

Lemma 1. *Let $H \subseteq G$ be Abelian groups. Assume that G/H is finitely generated. The following conditions are equivalent*:

1. *H splits in G.*
2. *The Abelian groups $G_{(n)}/H_{(n)}$ and $(G/H)_{(n)}$ are isomorphic for every $n \in \mathbb{Z}$.*
3. *$nG \cap H = nH$ for every $n \in \mathbb{Z}$.*

Proof. This result can be proven by standard techniques of Abelian groups and exact sequences. We only sketch the proof. The equivalence between 2 and 3 follows by showing the exactness of the sequence

$$\{0\} \to \frac{G_{(n)}}{H_{(n)}} \xrightarrow{j_n} \left(\frac{G}{H}\right)_{(n)} \xrightarrow{\pi_n} \frac{nG \cap H}{nH} \to \{0\},$$

where the maps j_n and π_n are defined as follows

$$j_n(g + H_{(n)}) := g + H, \qquad \pi_n(g + H) := ng + nH.$$

The fact that 1 implies 3 follows by noticing that, if $\pi : G \to G/H$ is the canonical quotient map and $p : G/H \to G$ is a splitting map, then for any $h = ng \in H$ we can define $h' := g - p(g + H)$. Since $\pi(h') = 0$ and since $nh' = ng$ we can argue that $ng \in nH$. This shows that $nG \cap H \subseteq nH$, while the other way is trivial.

For showing that 3 implies 1 we need the additional hypothesis that G/H is finitely generated, which, by the fundamental decomposition theorem for finitely generated Abelian groups, implies that G/H can be decomposed as the direct sum of a finite number of cyclic subgroups $G/H = C_1 \oplus \cdots \oplus C_k$. For each i select $l_i \in G$ as follows. If $C_i \simeq \mathbb{Z}$ and if $g_i + H$ is a generator of C_i, then let $l_i := g_i$. If $C_i \simeq \mathbb{Z}_{n_i}$ and if $g_i + H$ is a generator of C_i, then $n_i g_i \in H$ and by 3 this implies that there exists $h_i \in H$ such that $n_i g_i = n_i h_i$. In this case define $l_i := g_i - h_i$. Consider finally the subgroup L of G generated by $l_1, \ldots, l_k$. It is not difficult to verify that $G = H \oplus L$. □

2.2. Group codes over Laurent sequence groups

Let V be a finite Abelian group and let $V^{\mathbb{Z}}$ be the set of biinfinite sequences over V. If $v \in V^{\mathbb{Z}}$, $v(t)$ will denote the tth component of the sequence v. Let $\sigma : V^{\mathbb{Z}} \to V^{\mathbb{Z}}$ be the backward shift. If $I \subseteq \mathbb{Z}$, we denote by $_{|I} : V^{\mathbb{Z}} \to V^I$ the restriction operator to I so that, if $\mathscr{C} \subseteq V^{\mathbb{Z}}$, then $\mathscr{C}_{|I} \subseteq V^I$ denotes the set of the restrictions to I of all the sequences in $\mathscr{C}$.

In this paper we will consider only codes contained in the so called Laurent sequence group. A *Laurent sequence group* over a finite Abelian group V is defined as

$$\mathscr{L}_V := \{v \in V^{\mathbb{Z}} : \exists t \in \mathbb{Z} \text{ such that } v(k) = 0 \ \forall k \leqslant t\}.$$

This set inherits an Abelian group structure by a componentwise extension of the group operation in V and so it will be called *sequence group*.

In fact, if for any $r = \sum_{i=l}^{+\infty} r_i D^i \in \mathbb{Z}((D))$, we define the map

$$r(\sigma, \sigma^{-1}) : \mathscr{L}_V \to \mathscr{L}_V$$

by letting

$$(r(\sigma, \sigma^{-1})v)(t) := \left(\sum_{i=l}^{+\infty} r_i \sigma^{-i} v\right)(t) = \sum_{i=l}^{+\infty} r_i v(t-i), \tag{3}$$

$\mathscr{L}_V$ becomes a finitely generated $\mathbb{Z}((D))$-module.

We now come to the following fundamental definitions.

Definition 1 (*Controllability* [11, 23]). A subset $\mathscr{C} \subseteq \mathscr{L}_V$ is said to be *controllable* if, given any $v_1, v_2 \in \mathscr{C}$, there exists $n \in \mathbb{N}$ and $v \in \mathscr{C}$ such that

$$\begin{aligned} v_{|(-\infty,-1]} &= v_{1|(-\infty,-1]}, \\ v_{|[0,+\infty)} &= (\sigma^{-n} v_2)_{|[0,+\infty)}. \end{aligned} \tag{4}$$

Moreover, $\mathscr{C}$ is said to be *N-controllable* if (4) holds with fixed $n = N$ which is independent with the trajectories v_1, v_2. Finally, $\mathscr{C}$ is said to be *strongly controllable* if it is *N-controllable* for some $N \in \mathbb{N}$.

Definition 2 (*Completeness* [11, 23]). A subset $\mathscr{C} \subseteq \mathscr{L}_V$ is called *complete*, if, given any $v \in \mathscr{L}_V$, we have that

$$v_{|[t+1,t+n]} \in \mathscr{C}_{|[1,n]} \ \forall t \in \mathbb{Z}, \ \forall n \in \mathbb{N} \Rightarrow v \in \mathscr{C}. \tag{5}$$

Moreover, $\mathscr{C}$ is said to be *N-complete* if (5) holds with fixed $n = N$. Finally, $\mathscr{C}$ is said to be *strongly complete* if it is *N-complete* for some $N \in \mathbb{N}$.

A *group code* is a subgroup $\mathscr{C} \subseteq \mathscr{L}_V$ which is complete and σ-invariant, i.e., such that $\sigma\mathscr{C} = \mathscr{C}$. In other words a group code is a complete $\mathbb{Z}((D))$-submodule of $\mathscr{L}_V$.

The following proposition shows that a group code in our set up is automatically strongly complete and strongly controllable. This implies that the class of codes considered in [11,17] includes the codes analyzed in this paper.

Proposition 1 ([8], Lemma 3). *Let $\mathscr{C} \subseteq \mathscr{L}_V$ be a group code, where V is a finite Abelian group. Then $\mathscr{C}$ is strongly complete and strongly controllable.*

Let $\mathscr{C} \subseteq \mathscr{L}_V$ be a group code. For any $I \subseteq \mathbb{Z}$ we define the following subgroup of $\mathscr{C}$

$$\mathscr{C}_I := \{v \in \mathscr{C} | v(t) = 0 \ \forall t \notin I\}.$$

Let moreover

$$\mathscr{C}_f := \bigcup_{I \text{ finite}} \mathscr{C}_I$$

be the subgroup consisting of the sequences in $\mathscr{C}$ with finite support. We will also use the notation $\mathscr{C}_-$ and $\mathscr{C}_+$ for, respectively, $\mathscr{C}_{(-\infty,-1]}$ and $\mathscr{C}_{[0,+\infty)}$.

If $v \in \mathscr{L}_V$, define $v^-, v^+ \in \mathscr{L}_V$ by

$$\begin{aligned} (v^-)_{|(-\infty,-1]} &= v_{|(-\infty,-1]}, \quad & (v^-)_{|[0,+\infty)} &= 0, \\ (v^+)_{|(-\infty,-1]} &= 0, & (v^+)_{|[0,+\infty)} &= v_{|[0,+\infty)}. \end{aligned}$$

If $\mathscr{C} \subseteq \mathscr{L}_V$ is a group code, then we define

$$\mathscr{C}^+ := \{v^+ | v \in \mathscr{C}\}, \quad \mathscr{C}^- := \{v^- \mid v \in \mathscr{C}\}.$$

We clearly have that

$$\mathscr{C}_- \subseteq \mathscr{C}^-, \quad \mathscr{C}_+ \subseteq \mathscr{C}^+.$$

The *input group* of $\mathscr{C}$ is defined as

$$U(\mathscr{C}) := \mathscr{C}_{+|[0]}, \tag{6}$$

while the *state space* of $\mathscr{C}$ is defined as the quotient group

$$X(\mathscr{C}) := \frac{\mathscr{C}}{\mathscr{C}_- \oplus \mathscr{C}_+}. \tag{7}$$

It is a standard fact [11] that

$$X(\mathscr{C}) \simeq \frac{\mathscr{C}^+}{\mathscr{C}_+} \simeq \frac{\mathscr{C}^-}{\mathscr{C}_-}.$$

2.3. Shift operators

Let W and V be finite Abelian groups and let $\mathscr{C}_1 \subseteq \mathscr{L}_W$ and $\mathscr{C}_2 \subseteq \mathscr{L}_V$ be group codes. Any homomorphism $\psi : \mathscr{C}_1 \to \mathscr{C}_2$ which commutes with the shift σ

is called a *shift operator*. A shift operator ψ is said to be *causal* (resp. *anticausal*) if $\psi(\mathscr{C}_{1+}) \subseteq \mathscr{C}_{2+}$ (resp. $\psi(\mathscr{C}_{1-}) \subseteq (\mathscr{C}_{2-})$). Notice that a causal shift operator $\psi : \mathscr{C}_1 \to \mathscr{C}_2$ induces a natural homomorphism

$$\psi_U : U(\mathscr{C}_1) \to U(\mathscr{C}_2) \tag{8}$$

from the input group of $\mathscr{C}_1$ to the input group of $\mathscr{C}_2$.

A shift operator ψ is said to be *finitely anticipating* if there exists $l \in \mathbb{N}$ such that $\sigma^{-l} \circ \psi$ is causal and the minimal l for which this holds is called the *anticipation* of ψ. Finally, ψ is said to have *finite memory* if there exists $m \in \mathbb{N}$ such that $\sigma^m \psi$ is anticausal and the minimal m for which this holds is called the *memory* of ψ. A shift operator ψ is said to be *sliding window*, if there exist l and m and a homomorphism $\gamma : \mathscr{C}_{1|[-m,l]} \to V$ such that, given $w \in \mathscr{C}_1$,

$$\psi(w)(t) = \gamma(w_{|[-m+t,l+t]}) \quad \forall t \in \mathbb{Z}.$$

In this case we also use the notation γ^∞ for ψ. If $m = l = 0$, the shift operator is also called *static*. It is clear that γ^∞ has finite anticipation less than or equal to l and finite memory less than or equal to m. It can be shown that also the converse holds if $\mathscr{C}_1 = \mathscr{L}_W$. When this is not the case, we have a weaker result illustrated by the following proposition.

Proposition 2. *Let $\mathscr{C}_1 \subseteq \mathscr{L}_W$ and $\mathscr{C}_2 \subseteq \mathscr{L}_V$ be group codes and let $\psi : \mathscr{C}_1 \to \mathscr{C}_2$ be a shift operator. Then the following facts are equivalent*:

1. *ψ is finitely anticipating and finite memory.*
2. *ψ is sliding window.*
3. *$\psi(\mathscr{C}_{1f}) \subseteq \mathscr{C}_{2f}$.*

Proof. (2⇒3) is trivial.

(1⇒2) It follows from Proposition 1 that we can assume that $\mathscr{C}_1$ is M-complete for some $M \in \mathbb{N}$. Assume that ψ has finite anticipation l and finite memory m. Put $m^* := \max(m, M - l - 2)$. Consider $w_1, w_2 \in \mathscr{C}_1$ such that $w_{1|[-m^*,l]} = w_{2|[-m^*,l]}$. We now show that $\psi(w_1)(0) = \psi(w_2)(0)$ which will clearly imply that ψ is sliding window. Consider $w := w_1 - w_2$. Then, $w_{|[-m^*,l]} = 0$ and since $m^* \geqslant M - l - 2$ we have that $l + m^* + 1 \geqslant M - 1$. Hence, since $\mathscr{C}_1$ is M-complete, we can write $w = w^- + w^+$ where $w^- \in \sigma^{m^*}\mathscr{C}_{1-}$ and $w^+ \in \sigma^{-l-1}\mathscr{C}_{1+}$. Since ψ has finite anticipation l and finite memory m we have that

$$\psi(w^+) \in \psi(\sigma^{-l-1}\mathscr{C}_{1+}) = \sigma^{-1}\sigma^{-l}\psi(\mathscr{C}_{1+}) \subseteq \sigma^{-1}\mathscr{C}_{2+},$$
$$\psi(w^-) \in \psi(\sigma^{m^*}\mathscr{C}_{1-}) = \sigma^{m^*}\psi(\mathscr{C}_{1-}) \subseteq \sigma^m\psi(\mathscr{C}_{1-}) \subseteq \mathscr{C}_{2-}.$$

This yields

$$\psi(w)(0) = \psi(w^- + w^+)(0) = \psi(w^-)(0) + \psi(w^+)(0) = 0.$$

(3⇒1) Since $\mathscr{C}_1$ is a group code, then by Proposition 1 it is N-controllable for some $N \in \mathbb{N}$. This implies [11, strong controllability theorem, p. 1505] that each trajectory in $\mathscr{C}_{1(-\infty,0]}$ can be written as a finite sum of trajectories of support length at most $N+1$ and contained in $\mathscr{C}_{1(-\infty,0]}$. Now, it follows from condition 3 and from the fact that $\mathscr{C}_{1[0,N]}$ is finite that there exists $k \in \mathbb{N}$ such that $\psi(\mathscr{C}_{1[0,N]}) \subseteq \mathscr{C}_{2[-k,N+k]}$. This implies that

$$\psi(\mathscr{C}_{1(-\infty,0]}) \subseteq \mathscr{C}_{2(-\infty,k]}.$$

This shows that ψ has finite memory. The fact that ψ has finite anticipation can be shown in a similar way. □

Remark 1. From the proof of Proposition 2 it can be seen that, if $\psi : \mathscr{C}_1 \to \mathscr{C}_2$ is a shift operator with finite anticipation l and finite memory m and if $\mathscr{C}_1$ is M-complete, then there exists $\gamma_- : \mathscr{C}_{1|[-m^*,l]} \to V$ and $\gamma_+ : \mathscr{C}_{1|[-m,l^*]} \to V$ such that

$$\psi = \gamma_-^\infty = \gamma_+^\infty,$$

where $m^* := \max(m, M-l-2)$ and $l^* := \max(l, M-m-2)$.

Let $\psi : \mathscr{C}_1 \to \mathscr{C}_2$ be a shift operator. A *state space realization* of ψ is a quadruple (X, f, g, l), where X is a set called the *state space*, f and g are maps

$$f : X \times W \longrightarrow X,$$
$$g : X \times W \longrightarrow V$$

and where $l \in \mathbb{N}$ is called the *anticipation*, such that, given $w \in \mathscr{C}_1$ and $v \in \mathscr{C}_2$, we have that $\psi(w) = v$ if and only if there exists $x \in X^{\mathbb{Z}}$ for which the following relations hold

$$\begin{cases} x(k+1) = f(x(k), w(k)), \\ v(k-l) = g(x(k), w(k)) \end{cases} \tag{9}$$

for all $k \in \mathbb{Z}$. When the state space X is also an Abelian group and f and g are homomorphisms, (X, f, g, l) is called a *linear state space realization* of ψ.

It is well known [4–7,16,21] that, any causal shift operator $\psi : \mathscr{L}_W \to \mathscr{L}_V$ acting from a sequence group $\mathscr{L}_W$ to another sequence group $\mathscr{L}_V$ admits a linear state space realization, called canonical realization, with state space

$$X(\psi) := \frac{(\mathscr{L}_W)_-}{(\mathscr{L}_W)_- \cap \psi^{-1}(\mathscr{L}_V)_-}. \tag{10}$$

The canonical realization possesses an important minimality property. Indeed, if we consider another state space realization of ψ with state space X, there exists a surjective map $\pi : X_0 \to X(\psi)$, where $X_0 \subseteq X$. This shows that the cardinality of $X(\psi)$ must be less than or equal to the cardinality of the state space X.

Shift operators between Laurent sequences groups admit another nice algebraic representation. Let V and W be finite Abelian groups. An element $N = \sum_{i=l}^{+\infty} N_i D^i \in \mathrm{Hom}(W, V)((D))$ naturally induces a shift-invariant homomorphism

$$N(\sigma, \sigma^{-1}) : \mathscr{L}_W \to \mathscr{L}_V \tag{11}$$

by substituting the indeterminate D with the forward shift operator σ^{-1}. In other words the homomorphism $N(\sigma, \sigma^{-1})$ operates as follows

$$(N(\sigma, \sigma^{-1})w)(t) := \sum_{i=l}^{+\infty} N_i w(t-i) \tag{12}$$

for any $w \in \mathscr{L}_W$. A straightforward verification shows that every finitely anticipating shift operator between $\mathscr{L}_W$ and $\mathscr{L}_V$ is of the type above. Moreover, $N(\sigma, \sigma^{-1})$ has finite memory if and only if $N \in \mathrm{Hom}(W, V)[D, D^{-1}]$. In this case $N(\sigma, \sigma^{-1})$ is sliding window and it is also called a *polynomial shift operator*. On the other hand, causality for $N(\sigma, \sigma^{-1})$ corresponds to the fact that $N \in \mathrm{Hom}(W, V)[[D]]$ and therefore the causal polynomial shift operators are those for which $N \in \mathrm{Hom}(W, V)[D]$. There is another important concept we need to introduce. An element $N \in \mathrm{Hom}(W, V)((D))$ is said to be *rational* if there exist a $P \in \mathrm{Hom}(W, V)[D, D^{-1}]$ and a $r \in \mathbb{Z}[D, D^{-1}]$ having unitary trailing coefficient such that $rN = P$. If N is rational, $N(\sigma, \sigma^{-1})$ is said to be a *rational shift operator*. The importance of rational shift operators relies on the classical fact [4–7,16,21] that a shift operator over Laurent sequence groups is rational if and only if it admits a linear state space realization with a finite Abelian group as state space.

3. Encoders and inverters

Let $\mathscr{C} \subseteq \mathscr{L}_V$ be a group code. An *encoder* for $\mathscr{C}$ is an invertible finitely anticipating rational shift operator $\psi : \mathscr{L}_W \to \mathscr{C}$ for some finite Abelian group W. Finite anticipation insures that, at least in principle, the map can be implemented in real time with a finite delay. If ψ is, respectively, causal, polynomial, the encoder will be called, respectively, *causal, polynomial*. An encoder ψ, by definition, always admits the inverse $\psi^{-1} : \mathscr{C} \to \mathscr{L}_W$. In general, the only thing we can say is that ψ^{-1} is a homomorphism commuting with the shift. As we will see, many interesting coding and systems theoretic concepts regarding encoders can be defined or characterized through special properties of their inverses.

Given an encoder $\psi : \mathscr{L}_W \to \mathscr{C}$, an *inverter* for ψ consists of a triple $(\widetilde{W}, j, \phi)$, where

1. $\widetilde{W}$ is finite Abelian group called the *inverter group*,
2. $j : W \to \widetilde{W}$ is an injective homomorphism,
3. $\phi : \mathscr{L}_V \to \mathscr{L}_{\widetilde{W}}$ is a rational shift operator such that $\phi \circ \psi = j^{\infty}$.

In other words, an inverter is a shift operator between Laurent sequence groups whose restriction to $\mathscr{C}$ coincides with the inverse of the encoder. The following diagram summarizes the inverter definition.

$$\begin{array}{ccc} \mathscr{L}_W & \xrightarrow{\psi} & \mathscr{C} \\ {\scriptstyle j^\infty}\downarrow & & \downarrow{\scriptstyle i} \\ \mathscr{L}_{\widetilde{W}} & \xleftarrow{\phi} & \mathscr{L}_V \end{array}$$

where i is the canonical inclusion.

3.1. Noncatastrophic encoders

An encoder $\psi : \mathscr{L}_W \to \mathscr{C}$ is said to be *noncatastrophic* if

$$\psi^{-1}(\mathscr{C}_f) \subseteq (\mathscr{L}_W)_f,$$

in other words, by Proposition 2, if ψ^{-1} is sliding window.

It is a classical result that in the field case an encoder is noncatastrophic if and only if it admits a polynomial inverter. We will show that this fact holds true also for noncatastrophic encoders over finite Abelian groups.

In order to see this we need the following result which shows that a sliding window shift operator from a group code $\mathscr{C}$ to a Laurent sequence group $\mathscr{L}_V$ can be extended to a sliding window shift operator between Laurent sequence groups.

Proposition 3. *Let $\mathscr{C} \subseteq \mathscr{L}_V$ be a group code and let $\theta : \mathscr{C} \to \mathscr{L}_W$ be a sliding window shift operator. Then, there exist a finite Abelian group $\widehat{W}$, an injective homomorphism $\iota : W \to \widehat{W}$, and a polynomial shift operator $N(\sigma, \sigma^{-1}) : \mathscr{L}_V \to \mathscr{L}_{\widehat{W}}$, such that*

$$N(\sigma, \sigma^{-1})_{|\mathscr{C}} = \iota^\infty \circ \theta.$$

Moreover, $N(\sigma, \sigma^{-1})$ can be chosen to have the same anticipation and memory as θ.

Proof. Let $\gamma : \mathscr{C}_{|[-n,m]} \to W$ be such that $\gamma^\infty = \theta$. Consider the quotient group

$$\widehat{W} := \frac{V^{n+m+1} \times W}{H},$$

where

$$H := \big\{(v, w) \in V^{n+m+1} \times W | v \in \mathscr{C}_{|[-n,m]},\ \gamma(v) = w\big\}.$$

Let $\hat{\gamma} : V^{n+m+1} \to \widehat{W}$ be given by $\hat{\gamma}(v) = (-v, 0) + H$. Moreover, let $\iota : W \to \widehat{W}$ be given by $\iota(w) = (0, w) + H$. The map ι is clearly injective and we have that

$$\hat{\gamma}_{|\mathscr{C}_{|[-n,m]}} = \iota \circ \gamma. \tag{13}$$

Put $N(\sigma, \sigma^{-1}) := \hat{\gamma}^\infty$: it is clear that this is a sliding window shift operator from $\mathscr{L}_V$ to $\mathscr{L}_{\widehat{W}}$ (hence a polynomial shift operator), with the required properties. □

Remark 2. Unfortunately, the Abelian group $\widehat{W}$ introduced in the previous proposition may be very big. This group can be reduced in the following way. Let $n \in$

$\mathbb{N}$ be such that $nW = 0 = nV$. Using the fundamental decomposition theorem [13, Theorem 2.1 in Chapter II] we can write

$$W = C_1 \oplus \cdots \oplus C_k,$$

where C_i is a cyclic subgroup of W of order n_i, with $n_i | n$. Define $\overline{W} := (\mathbb{Z}_n)^k$ and let $\bar{\iota} : W \to \overline{W}$ be the map sending the generator of C_i to $(0, \ldots, 1, \ldots, 0)$ (with 1 at the ith position). Clearly, also the Abelian group $\widehat{W}$ introduced in the previous proposition can be decomposed as

$$\widehat{W} = C'_1 \oplus \cdots \oplus C'_h,$$

where C'_i is a cyclic subgroup of $\widehat{W}$ of order m_i with $m_i | n$. Consider as before $\overline{\widehat{W}} := (\mathbb{Z}_n)^h$ and let $\bar{\kappa} : \widehat{W} \to \overline{\widehat{W}}$ be defined analogously to $\bar{\iota}$. It is easy to see that there exists an injective homomorphism $\kappa : \overline{W} \to \overline{\widehat{W}}$ such that the following diagram commutes

$$\begin{array}{ccc} W & \xrightarrow{\iota} & \widehat{W} \\ \downarrow \bar{\iota} & & \downarrow \bar{\kappa} \\ \overline{W} & \xrightarrow{\kappa} & \overline{\widehat{W}} \end{array} \tag{14}$$

where ι is the homomorphism introduced in the previous proposition. Since all the groups involved are actually $\mathbb{Z}_n$-modules and $\overline{W}$ is $\mathbb{Z}_n$-free, it follows that the injection κ splits, i.e., there exists $\zeta : \overline{\widehat{W}} \to \overline{W}$ such that $\zeta \circ \kappa = \mathrm{id}_{\overline{W}}$. Now, consider the homomorphism

$$\tilde{\gamma} := \zeta \circ \bar{\kappa} \circ \hat{\gamma} : V^{n+m+1} \to \overline{W},$$

where $\hat{\gamma}$ is the homomorphism defined in the proof of the previous proposition. Then, it follows from (13) and (14) that

$$\tilde{\gamma}_{|\mathscr{C}_{|[-n,m]}} = \zeta \circ \bar{\kappa} \circ \hat{\gamma}_{|\mathscr{C}_{|[-n,m]}} = \zeta \circ \bar{\kappa} \circ \iota \circ \gamma = \zeta \circ \kappa \circ \bar{\iota} \circ \gamma = \bar{\iota} \circ \gamma.$$

This implies that $N(\sigma, \sigma^{-1}) = \tilde{\gamma}^{\infty}$ provides an inverter.

Observe finally that, while $\widehat{W}$ depends also on V, the number of generators k of $\overline{W}$ depends only on the group W.

We can now state the following result which is direct consequence of Proposition 2, Proposition 3, and Remark 2.

Corollary 1. *Let $\mathscr{C} \subseteq \mathscr{L}_V$ be a group code and let $\psi : \mathscr{L}_W \to \mathscr{C}$ be an encoder for it. Then, the following conditions are equivalent*

1. *ψ is noncatastrophic.*
2. *The inverse of ψ is sliding window.*
3. *ψ admits a polynomial inverter.*

Moreover, if n is a number such that $nW = 0 = nV$ and W is generated by k elements, then the inverter group of the polynomial inverter in 3 *can be chosen to be* $\widetilde{W} = \mathbb{Z}_n^k$.

3.2. Minimal encoders

Let $\mathscr{C} \subseteq \mathscr{L}_V$ be a group code and let $\psi : \mathscr{L}_W \to \mathscr{C}$ be a causal encoder for it. Let $X(\mathscr{C})$ be the state space of $\mathscr{C}$ introduced in (7) and let $X(\psi)$ be the state space of the canonical realization of ψ defined in (10). Consider the homomorphism

$$\psi_X : X(\psi) \to X(\mathscr{C})$$

defined as follows: if $x \in X(\psi)$ and $w \in (\mathscr{L}_W)_-$ is any of its representatives, then we define

$$\psi_X(x) := \psi(w) + (\mathscr{C}_- \oplus \mathscr{C}_+).$$

It can be shown that ψ_X is a well-defined surjective homomorphism [20]. These considerations motivate the following definition.

Definition 3. A causal encoder ψ is said to be *minimal* if the homomorphism ψ_X defined above is an isomorphism.

We have the following characterization of minimal encoders which sharpen [17, Proposition 6.1].

Proposition 4. *Let $\psi : \mathscr{L}_W \to \mathscr{C}$ be a causal encoder. The following conditions are equivalent*:

1. *ψ is minimal.*
2. *$w \in (\mathscr{L}_W)_-$ and $\psi(w) \in \mathscr{C}_- \oplus \mathscr{C}_+ \Rightarrow \psi(w) \in \mathscr{C}_-$.*
3. *ψ^{-1} is a sliding window causal and anticausal shift operator.*

Proof

(1⇔2) It follows from the definition of ψ_X.

(2⇒3) Let $v \in \mathscr{C}_-$ and let $w \in \mathscr{L}_W$ be such that $\psi(w) = v$. Write $w = w^- + w^+$ with $w^- \in (\mathscr{L}_W)_-$ and $w^+ \in (\mathscr{L}_W)_+$. Then,

$$\psi(w^-) = v - \psi(w^+) \in \mathscr{C}_- \oplus \mathscr{C}_+.$$

By condition 2 this implies that $\psi(w^-) \in \mathscr{C}_-$ which yields $\psi(w^+) = 0$ and hence $w^+ = 0$. This shows that ψ^{-1} is anticausal. Let now $v \in \mathscr{C}_+$ and let $w \in \mathscr{L}_W$ be such that $\psi(w) = v$. Decomposing $w = w^- + w^+$ as above, we can argue that

$$\psi(w^-) = v - \psi(w^+) \in \mathscr{C}_+.$$

By condition 2 this implies that $\psi(w^-) \in \mathscr{C}_-$ and so we can argue that $\psi(w^-) = 0$ and hence $w^- = 0$, showing in this way that ψ^{-1} is causal. Finally using Proposition 2 we can argue that ψ^{-1} is sliding window.

(3⇒2) Let $w \in (\mathscr{L}_W)_-$ be such that $\psi(w) = v^- + v^+$ with $v^- \in \mathscr{C}_-$ and $v^+ \in \mathscr{C}_+$. Then,

$$w = \psi^{-1}(v^-) + \psi^{-1}(v^+)$$

and since ψ^{-1} is causal and anticausal, it follows that $\psi^{-1}(v^+) = 0$ and thus $v^+ = 0$, which yields $\psi(w) \in \mathscr{C}_-$. □

From Remark 1 there exist maps

$$\gamma_- : \mathscr{C}_{|[-M+2,0]} \to W, \quad \gamma_+ : \mathscr{C}_{|[0,M-2]} \to W$$

such that $\psi^{-1} = \gamma_-^\infty = \gamma_+^\infty$, where M is such that $\mathscr{C}$ is M-complete. Using Proposition 3 it follows that a minimal encoder admits both a causal polynomial inverter and an anticausal polynomial inverter. This generalizes a well known result which has been proved in the field case in [9,14].

3.3. Systematic encoders

Another important class of encoders is constituted by the systematic encoders, which are encoders admitting static inverters.

Definition 4. A causal encoder $\psi : \mathscr{L}_W \to \mathscr{C}$ is said to be *systematic* if there exists a surjective homomorphism $\pi : V \to W$ such that π^∞ is the left inverse of ψ. The encoder is called *essentially systematic* if π is only defined on $\mathscr{C}_{|[0]}$.

Notice from the definition that a systematic encoder is necessarily essentially systematic. Notice moreover that systematicity is equivalent to the existence of a static inverter having as inverter group W itself. The previous definition is an abstract version of the definition which is commonly proposed in the literature. Indeed, it is not difficult to verify that the map

$$p : W \to V,$$
$$a \mapsto p(a) := \psi(\delta_a)_{|[0]},$$

where $\delta_a \in \mathscr{L}_W$ is such that $\delta_a(0) = a$ and $\delta_a(k) = 0$ for $k \neq 0$, is a splitting map for π, i.e., $\pi \circ p = \mathrm{id}_W$. This implies that

- $V = V_1 \oplus V_2$, where $V_1 := \ker \pi$ and $V_2 := \mathrm{im}\, p$;
- the splitting map $p : W \to V_2$ is an isomorphism;
- by defining the shift operator $\psi_1 := (\mathrm{id}_V - p \circ \pi)^\infty \circ \psi$ from $\mathscr{L}_W$ to $\mathscr{L}_{V_1}$, we have that the encoder ψ can be represented as a map

$$\psi : \mathscr{L}_W \to \mathscr{L}_{V_1} \oplus \mathscr{L}_{V_2},$$
$$w \mapsto \psi(w) = \psi_1(w) + p^\infty(w).$$

Example. Let $\psi : \mathscr{L}_W \to \mathscr{L}_V$ be a causal shift operator. Consider the graph of ψ

$$\mathscr{G}(\psi) \subseteq \mathscr{L}_W \oplus \mathscr{L}_V.$$

Clearly, $\mathscr{G}(\psi)$ is a group code and it has a systematic encoder

$$\phi : \mathscr{L}_W \to \mathscr{G}(\psi),$$
$$w \mapsto \phi(w) := \begin{pmatrix} w \\ \psi(w) \end{pmatrix}.$$

In this case the map $\pi : W \oplus V \to W$ is simply the projection on the first factor.

Corollary 2. *Any essentially systematic encoder is minimal*.

Proof. It follows from condition 3 of Proposition 4. □

The following is a converse to Corollary 2 in a very special case.

Corollary 3. *Let $\mathscr{C} \subseteq \mathscr{L}_V$ be a* 2*-complete group code*. *Then*, *any minimal causal encoder for $\mathscr{C}$ must be essentially systematic*.

Proof. Let ψ be a minimal causal encoder for $\mathscr{C}$. It follows from condition 3 of Proposition 4 that ψ^{-1} is a causal and anticausal sliding window map. Hence, by Remark 1 after Proposition 2, it follows that ψ^{-1} is static. This implies that ψ is essentially systematic. □

4. Group codes and their encoders

It is well-known [11,15,19,20] that not every group code admits a minimal or a systematic encoder. The solution proposed in [11,17] consists in taking into consideration nonlinear encoders, i.e. encoders which are not homomorphisms. However, as mentioned in the introduction, in some situations it may be more convenient to restrict to the class of linear encoders. In this section it will be analyzed how much the class of codes is restricted by imposing the existence of encoders with particular properties.

First observe that in our context a group code $\mathscr{C} \subseteq \mathscr{L}_V$ always admits a rational encoder as the following theorem points out. For this reason in our set up group codes are also called convolutional codes, since the encoding process consists in a convolution.

Theorem 1 ([8], Lemma 3; [7], Theorems 1, 2 and 5). *Let $\mathscr{C} \subseteq \mathscr{L}_V$ be a σ-invariant subgroup of $\mathscr{L}_V$. The following conditions are equivalent*:

1. *$\mathscr{C}$ is a group code*.
2. *There exists an encoder $\psi : \mathscr{L}_W \to \mathscr{C}$ for $\mathscr{C}$*.

3. *The canonical state space $X(\mathscr{C})$ of $\mathscr{C}$ is a finite Abelian group*.

Moreover, if any of the above conditions is satisfied, then $\mathscr{C}$ admits a causal polynomial encoder. Finally the finite Abelian group W introduced in point 2 *is uniquely determined by $\mathscr{C}$*.

Remark 3. The finite Abelian group W introduced in the previous theorem will be called the *encoding group* of $\mathscr{C}$ and will be denoted by the symbol $W(\mathscr{C})$. It has been shown in [7, Proposition 1] that the input group $U(\mathscr{C})$ introduced in (6) and the encoding group $W(\mathscr{C})$ have the same cardinality. However in general they are not isomorphic.

4.1. Group codes admitting causal encoders with causal inverse

It can be seen that a group code $\mathscr{C}$ always admits a causal encoder or an encoder with causal inverse, but does not admit in general an encoder which is simultaneously causal and has causal inverse. The following result shows, in particular, that a group code $\mathscr{C}$ admits such an encoder if and only if the groups $U(\mathscr{C})$ and $W(\mathscr{C})$ are isomorphic.

Theorem 2. *Let $\mathscr{C} \subseteq \mathscr{L}_{\mathbb{V}}$ be a group code. Then the following conditions are equivalent*:

1. *$\mathscr{C}$ admits a causal encoder with a causal inverse*.
2. *$U(\mathscr{C})$ and $W(\mathscr{C})$ are isomorphic*.
3. *$U(\mathscr{C}_{(n)}) = U(\mathscr{C})_{(n)}$ for all $n \in \mathbb{Z}$*.
4. *$nU(\mathscr{C}) = U(n\mathscr{C})$ for all $n \in \mathbb{Z}$*.
5. *$(n\mathscr{C})_+ = n(\mathscr{C}_+)$ for all $n \in \mathbb{Z}$*.
6. *$0 \to \sigma^{-1}(\mathscr{C}_+) \to \mathscr{C}_+ \to U(\mathscr{C}) \to 0$ splits*.

Moreover, if any of the previous conditions holds true, then the encoder of point 1 *can be chosen to be polynomial*.

Proof. (1⇒2) This is direct consequence of (8).

(2⇒4) It follows from 2 that $nU(\mathscr{C}) \simeq nW(\mathscr{C}) \simeq W(n\mathscr{C})$. On the other hand, as observed in Remark 3, $W(n\mathscr{C})$ and $U(n\mathscr{C})$ have the same cardinality, therefore also $nU(\mathscr{C})$ and $U(n\mathscr{C})$ have the same cardinality. Since we also have the obvious inclusion $nU(\mathscr{C}) \subseteq U(n\mathscr{C})$, this implies that they are indeed equal.

(4⇒5) Notice that $\supseteq$ is always true. We need to prove $\subseteq$. Let $v \in \mathscr{C}$ be such that $nv \in \mathscr{C}_+$. Then, $x := (nv)(0) \in U(n\mathscr{C})$ and it follows from 4 that there exists $\tilde{v}_0 \in \mathscr{C}_+$ such that $(n\tilde{v}_0)(0) = x$. Notice now that $n(v - \tilde{v}_0) \in \sigma^{-1}(n\mathscr{C})_+$. By

repeating this argument we can construct by induction elements $\tilde{v}_k \in \sigma^{-k}\mathscr{C}_+$ such that

$$n(v - \tilde{v}_0 - \cdots - \tilde{v}_k) \in \sigma^{-(k+1)}(n\mathscr{C})_+ \quad \forall k \in \mathbb{N}.$$

Consider now

$$\tilde{v} := \sum_{k=0}^{+\infty} \tilde{v}_k.$$

Notice that $nv = n\tilde{v}$. Moreover, since $\mathscr{C}$ is complete, $\tilde{v} \in \mathscr{C}_+$. This shows that $nv \in n(\mathscr{C}_+)$.

(5⇒3) Notice that $\subseteq$ is always true. We need to prove $\supseteq$. Let $x \in U(\mathscr{C})_{(n)}$ and let $v \in \mathscr{C}_+$ be such that $v(0) = x$. Then

$$\sigma(nv) = n\sigma(v) \in (n\mathscr{C})_+.$$

It then follows from 5 that there exists $\tilde{v} \in \mathscr{C}_+$ such that $n\tilde{v} = n\sigma v$. Hence, $v - \sigma^{-1}\tilde{v} \in (\mathscr{C}_{(n)})_+$ and $(v - \sigma^{-1}\tilde{v})(0) = v(0) = x$. This shows that $x \in U(\mathscr{C}_{(n)})$.

(3⇒6) It follows from Lemma 1 that it is sufficient to show that

$$n(\mathscr{C}_+) \cap \sigma^{-1}(\mathscr{C}_+) \subseteq n\sigma^{-1}(\mathscr{C}_+).$$

Let $v \in \mathscr{C}_+$ be such that $nv \in \sigma^{-1}(\mathscr{C}_+)$. This implies that $v(0) \in U(\mathscr{C})_{(n)}$. It follows from 3 that there exists $\tilde{v} \in \mathscr{C}_{(n)+}$ such that $\tilde{v}(0) = v(0)$. Then,

$$nv = n(v - \tilde{v}) \in n\sigma^{-1}(\mathscr{C}_+).$$

(6⇒1) Let $U := U(\mathscr{C})$ and let $\theta : U \to \mathscr{C}_+$ be a splitting homomorphism for the exact sequence in 6, i.e., a homomorphism such that $(\theta(x))(0) = x$ for all $x \in U$. Define $\psi : \mathscr{L}_U \to \mathscr{C}$ by letting

$$\psi(u) := \sum_{t=0}^{+\infty} \sigma^{-t}\theta(u(t))$$

for every $u \in \mathscr{L}_U$. Completeness insures that $\psi(u)$ defined above is indeed in $\mathscr{C}$ and ψ is clearly a causal shift operator.

We now show that ψ is invertible. Let $u \in \mathscr{L}_U \setminus \{0\}$ and let $t \in \mathbb{Z}$ be such that $u(t) \neq 0$ and $u(s) = 0$ for all $s < t$. Then, $\psi(u)(t) = \theta(u(t))(t) = u(t) \neq 0$. This proves injectivity. We want to prove now the surjectivity. Let $v \in \mathscr{C}$. By σ-invariance it is not restrictive to assume that $v \in \mathscr{C}_+$. Define $u \in (\mathscr{L}_U)_+$ in the following recursive way:

$$u(0) = v(0), \tag{15}$$

$$u(t) = \left(v - \sum_{s=0}^{t-1} \sigma^{-s}\theta(u(s)) \right)(t) \quad t \geqslant 1. \tag{16}$$

We have to prove first that $u(t)$ determined in this way are actually in U. This will be proved by induction. Clearly, $u(0) \in U$. Suppose we know that $u(0), u(1), \ldots,$

$u(t-1)$ are in U and satisfy (16). By (16), in order to show that $u(t) \in U$, it is enough to prove that

$$\left(v - \sum_{s=0}^{t-1} \sigma^{-s}\theta(u(s)) \right)_{|(-\infty,t-1]} = 0.$$

Observe preliminarily that

$$\left(v - \sum_{s=0}^{t-1} \sigma^{-s}\theta(u(s)) \right)_{|(-\infty,-1]} = 0.$$

On the other hand, if $0 \leqslant \tau \leqslant t-1$, then

$$\begin{aligned}\left(v - \sum_{s=0}^{t-1} \sigma^{-s}\theta(u(s)) \right)(\tau) &= \left(v - \sum_{s=0}^{\tau-1} \sigma^{-s}\theta(u(s)) \right)(\tau) - \theta(u(\tau))(0) \\ &= u(\tau) - u(\tau) = 0.\end{aligned}$$

This reasoning proves also that $v = \psi(u)$. Moreover, the fact that $u \in (\mathscr{L}_U)_+$ proves that the inverse is causal. Notice that we have not actually shown that ψ is an encoder since we have not proven rationality of ψ. Hence we have not proven 1 yet. However, it is easy to realize that rationality is not used in the implication (1⇒2) so that we can be sure that conditions 2–6 are equivalent. We will now complete the proof by showing that these conditions imply the existence of a causal polynomial encoder with causal inverse for $\mathscr{C}$. Let us go back to the way we have constructed the map ψ starting from the splitting map θ. It is clear that if θ has codomain in $\mathscr{C}_{[0,m]}$, for some $m \in \mathbb{N}$, then the resulting map ψ is a sliding window shift operator, hence polynomial. So the key point is to show that a splitting map θ, for the exact sequence in 6, can be found with codomain in $\mathscr{C}_{[0,m]}$. This will be done by showing that we can find $m \in \mathbb{N}$ such that

$$U(\mathscr{C}) = \mathscr{C}_{[0,m]|[0]} \tag{17}$$

and that the following exact sequence

$$0 \to \mathscr{C}_{[1,m]} \to \mathscr{C}_{[0,m]} \to \mathscr{C}_{[0,m]|[0]} \to 0 \tag{18}$$

splits. Indeed, a splitting map of this exact sequence, will also be a splitting map of the exact sequence in 6 and by construction will have codomain in $\mathscr{C}_{[0,m]}$.

To show (17), suppose that $x \in U(\mathscr{C})$ and let $v \in \mathscr{C}_+$ such that $v(0) = x$. Then $v = \phi(w)$ for some $w \in \mathscr{L}_W$. Let $w' \in \mathscr{L}_W$ such that $w'_{|(-\infty,0]} = w_{|(-\infty,0]}$ and that $w'_{|[1,+\infty)} = 0$. If we define $v' := \phi(w') \in \mathscr{C}$, it is not difficult to check that $v'(0) = v(0) = x$ and that $v' \in \mathscr{C}_{[0,m]}$. To show that (18) splits, it is enough to show, by virtue of Lemma 1 that

$$n(\mathscr{C}_{[0,m]}) \cap (\mathscr{C}_{[1,m]}) = n(\mathscr{C}_{[1,m]})$$

for all $n \in \mathbb{Z}$. The inclusion $\supseteq$ is trivial. Suppose conversely that $v \in \mathscr{C}_{[0,m]}$ and that $nv \in \mathscr{C}_{[1,m]}$. This means that $nv(0) = 0$ and so, by condition 3, there exists

$\tilde{v} \in (\mathscr{C}_{(n)})_+$ such that $v(0) = \tilde{v}(0)$. So there exists $\tilde{w} \in \mathscr{L}_W$ such that $\tilde{v} = \phi(\tilde{w})$. Define as above $\tilde{w}' \in \mathscr{L}_W$ such that $\tilde{w}'_{|(-\infty,0]} = \tilde{w}_{|(-\infty,0]}$ and that $\tilde{w}'_{|[1,+\infty)} = 0$ and $\tilde{v}' := \phi(\tilde{w}')$. Observe that $\tilde{v}' \in \mathscr{C}_{[0,m]}$, $n\tilde{v}' = 0$ and that $\tilde{v}'(0) = \tilde{v}(0) = v(0)$. This implies that $v - \tilde{v}' \in \mathscr{C}_{[1,m]}$ and that $nv = n(v - \tilde{v}')$. This completes the proof. □

4.2. Minimal group codes

In this section we will introduce the concepts of minimal and of systematic group codes. Then, the properties of these group codes will be investigated and compared.

Definition 5. A group code is said to be *minimal* if it admits a minimal encoder. A group code is said to be *(essentially) systematic* if it admits an (essentially) systematic encoder.

A direct consequence of Proposition 4 is that, if a group code is minimal, then it admits a causal encoder with causal inverse and moreover that if a group code is systematic, then it is minimal. This considerations imply that both for minimal and for systematic group codes we have that the encoding group and the input group coincide.

We give now a theorem which provides a characterization of minimal group codes.

Theorem 3. *Let $\mathscr{C} \subseteq \mathscr{L}_V$ be a group code. The following conditions are equivalent*:

1. *$\mathscr{C}$ is minimal.*
2. *The exact sequence $\{0\} \to \mathscr{C}_+ \to \mathscr{C}^+ \to X(\mathscr{C}) \to \{0\}$ splits.*
3. *$n(\mathscr{C}^+) \cap \mathscr{C}_+ = n(\mathscr{C}_+)$ for all $n \in \mathbb{Z}$.*
4. *$(\mathscr{C}^-)_{(n)} = (\mathscr{C}_{(n)})^-$ for all $n \in \mathbb{Z}$.*

Proof. (2⇔3) This follows from Lemma 1.

(3⇔4) This follows from a straightforward verification.

(1⇒2) Let $\psi : \mathscr{L}_W \to \mathscr{C}$ be a minimal encoder. Define $\theta : \mathscr{C}^+ \to \mathscr{C}_+$ as follows: given $z \in \mathscr{C}^+$, let $v \in \mathscr{C}$ be any sequence such that $v^+ = z$. Put $\theta(z) := \psi(\psi^{-1}(v)^+)$. Since ψ is causal, $\theta(z)$ is in $\mathscr{C}_+$, and since ψ^{-1} is anticausal, the value of $\theta(z)$ does not depend on the choice of v. Therefore θ is a well-defined homomorphism. Now, if $z \in \mathscr{C}_+$, we can take $v = z$ and, since ψ^{-1} is causal, $\psi^{-1}(v)^+ = \psi^{-1}(v)$ and therefore $\theta(z) = z$. This proves that θ is a splitting map for the exact sequence in 2.

(2⇒1) Let $\theta : \mathscr{C}^+ \to \mathscr{C}_+$ be a splitting map for the exact sequence in 2, i.e., a homomorphism from $\mathscr{C}^+$ to $\mathscr{C}_+$ which is the identity map when restricted to $\mathscr{C}_+$. Consider the map

$$\phi : \mathscr{C} \to \mathscr{L}_{U(\mathscr{C})}$$

defined by

$$\phi(v)(t) := \theta((\sigma^t v)^+)(0).$$

The map ϕ is clearly anticausal. It is also causal. Indeed, assume that $v \in \mathscr{C}_+$. Then, for every $t < 0$ we have that $\sigma^t v \in \mathscr{C}_+$ and therefore

$$\phi(v)(t) = \theta(\sigma^t v)(0) = (\sigma^t v)(0) = v(t) = 0.$$

We now show that ϕ is invertible. Let $v \in \mathscr{C}$ be such that $\phi(v) = 0$ and assume by contradiction that $v \neq 0$. It is not restrictive to assume that $v \in \mathscr{C}_+$ and that $v(0) \neq 0$. Then, $\phi(v)(0) = \theta(v^+)(0) = \theta(v)(0) = v(0) \neq 0$ which would show that $\phi(v) \neq 0$. This proves injectivity. Regarding surjectivity, fix a $u \in (\mathscr{L}_{U(\mathscr{C})})_+$. For each $t \geqslant 0$ choose inductively $v_t \in \sigma^{-t}\mathscr{C}_+$ such that

$$\begin{cases} v_0(0) = u(0), \\ v_t(t) = u(t) - \sum_{s=0}^{t-1} \theta((\sigma^t v_s)^+)(0), \quad t \geqslant 1 \end{cases}$$

and define $v := \sum_{t=0}^{+\infty} v_t$. Then

$$\phi(v)(t) = \sum_{s=0}^{t} \phi(v_s)(t) = \sum_{s=0}^{t} \theta((\sigma^t v_s)^+)(0) = v_t(t) + \sum_{s=0}^{t-1} \theta((\sigma^t v_s)^+)(0) = u(t).$$

This also proves that $\psi := \phi^{-1} : \mathscr{L}_{U(\mathscr{C})} \to \mathscr{C}$ is a causal shift operator with causal and anticausal inverse ϕ. It remains to show that ψ is rational. By observing that Proposition 4 holds true also for general nonrational shift operators, we can argue that the canonical state space $X(\psi)$ of ψ is isomorphic to the canonical state space $X(\mathscr{C})$ of $\mathscr{C}$. By Theorem 1 this implies that $X(\psi)$ is a finite Abelian group and so ψ must be rational. □

Remark 4. The existence of a homomorphic minimal encoder has already been studied in a slightly different set up in [17]. In that paper the notion of encoder is given directly as a state space realization and the existence of a homomorphic minimal encoder has been shown to be equivalent to the fact that input group $U(\mathscr{C})$ of the code $\mathscr{C}$ splits in the canonical branch group $B(\mathscr{C})$ of the code, which is defined as

$$B(\mathscr{C}) := \{([v], v_{|[0]}, [\sigma^{-1}v]) : v \in \mathscr{C}\},$$

where $[v] \in X(\mathscr{C})$ denotes the coset of the representative v. It can be shown that $U(\mathscr{C})$ splits in $B(\mathscr{C})$ if and only if $\mathscr{C}_+$ splits in $\mathscr{C}^+$. It is interesting to notice that this is true also in the general nonabelian case and this fact suggests that the equivalence of conditions 1 and 2 of the previous theorem holds true more in general.

We can deepen the structural analysis of minimal group codes by observing the following fact.

Lemma 2. *Let $\mathscr{C} \subseteq \mathscr{L}_V$ be a group code and $n \in \mathbb{Z}$. The following conditions are equivalent.*

1. $n(\mathscr{C}^+) \cap \mathscr{C}_+ = n(\mathscr{C}_+)$.
2. (a) $(n\mathscr{C})_+ = n(\mathscr{C}_+)$,
   (b) $n\mathscr{C} \cap (\mathscr{C}_- \oplus \mathscr{C}_+) = (n\mathscr{C})_- \oplus (n\mathscr{C})_+$.

Proof. (1⇒2) (a) follows directly. As far as (b) we only have to show $\subseteq$. Let $v \in \mathscr{C}$ be such that $nv = \tilde{v}^- + \tilde{v}^+$, with $\tilde{v}^- \in \mathscr{C}_-$ and $\tilde{v}^+ \in \mathscr{C}_+$. Since $\tilde{v}^+ \in n(\mathscr{C}^+)$, it follows from 1 that there exists $v' \in \mathscr{C}_+$ such that $\tilde{v}^+ = nv'$. Hence we can argue that

$$\tilde{v}^+ \in n(\mathscr{C}_+) \subseteq (n\mathscr{C})_+.$$

On the other hand observe that

$$\tilde{v}^- = nv - \tilde{v}^+ \in n\mathscr{C} \cap \mathscr{C}_- = (n\mathscr{C})_-.$$

(2⇒1) Let $z \in \mathscr{C}^+$ be such that $nz \in \mathscr{C}_+$. Let $v \in \mathscr{C}$ be such that $v^+ = z$. Since $(nv)^+ \in \mathscr{C}_+$ we have that $nv \in \mathscr{C}_- \oplus \mathscr{C}_+$. It follows from (b) that there exist $\tilde{v}_1, \tilde{v}_2 \in \mathscr{C}$ such that $n\tilde{v}_1 \in (n\mathscr{C})_-$, $n\tilde{v}_2 \in (n\mathscr{C})_+$ and $nv = n\tilde{v}_1 + n\tilde{v}_2$. It now follows from (a) that that there exists $v' \in \mathscr{C}_+$ such that $n\tilde{v}_2 = nv'$. Notice now that $nz = nv' \in n(\mathscr{C}_+)$. □

From the previous lemma we can prove the following further characterization of minimal group codes.

Corollary 4. *Let $\mathscr{C} \subseteq \mathscr{L}_V$ be a group code. The following conditions are equivalent*:

1. *$\mathscr{C}$ is minimal.*
2. *$U(n\mathscr{C}) = nU(\mathscr{C})$ and $X(n\mathscr{C}) = nX(\mathscr{C})$ for all $n \in \mathbb{Z}$.*

Proof. By Theorem 3 we have that 1 is equivalent to the fact that $n(\mathscr{C}^+) \cap \mathscr{C}_+ = n(\mathscr{C}_+)$ for all $n \in \mathbb{Z}$, which, by Lemma 2, is equivalent to the fact that $(n\mathscr{C})_+ = n(\mathscr{C}_+)$, and $n\mathscr{C} \cap (\mathscr{C}_- \oplus \mathscr{C}_+) = (n\mathscr{C})_- \oplus (n\mathscr{C})_+$ for all $n \in \mathbb{Z}$. By Theorem 2, the first of the previous two conditions is equivalent to the fact that $U(n\mathscr{C}) = nU(\mathscr{C})$ for all $n \in \mathbb{Z}$, while, by a straightforward verification, it can be shown that the second condition is equivalent to the fact that $X(n\mathscr{C}) = nX(\mathscr{C})$ for all $n \in \mathbb{Z}$. □

4.3. Systematic group codes

The following theorem provides a characterization of systematic group codes. A similar condition has been proposed also in [19].

Theorem 4. *Let $\mathscr{C} \subseteq \mathscr{L}_V$ be a group code. The following conditions are equivalent*:

1. *$\mathscr{C}$ is systematic.*
2. *$\mathscr{C}$ admits a causal encoder $\psi : \mathscr{L}_W \to \mathscr{C}$ which has a causal inverter with inverter group W.*
3. *The input group $U(\mathscr{C})$ splits in V.*

Proof. (1⇒2) This is obvious since a systematic encoder admits a static inverter with inverter group W.

(2⇒3) Let $\phi : \mathscr{L}_V \to \mathscr{L}_W$ be a causal inverter with inverter group W for ψ. Consider the maps ψ_U and ϕ_U defined from ψ and ϕ as done in (8). Then $\theta := \psi_U \circ \phi_U$ is a homomorphism from V to $U(\mathscr{C})$. Let j denote the inclusion map of $U(\mathscr{C})$ inside V. Let $a \in U(\mathscr{C})$ and let $v \in \mathscr{C}_+$ such that $v(0) = a$. Then

$$(\theta \circ j)(a) = \theta(a) = \psi_U \circ \phi_U(a) = ((\psi \circ \phi)(v))(0) = v(0) = a$$

which shows that that $\theta \circ j = \mathrm{id}_{U(\mathscr{C})}$. This implies that $U(\mathscr{C})$ splits in V.

(3⇒1) From the splitting map $\theta : V \to U(\mathscr{C})$ we can define the static shift operator

$$\phi := \theta^{\infty}_{|\mathscr{C}} : \mathscr{C} \to \mathscr{L}_{U(\mathscr{C})}.$$

We want to prove that ϕ is invertible. Let $v \in \mathscr{C}$ be such that $\phi(v) = 0$ and assume by contradiction that $v \neq 0$. It is not restrictive to assume that $v \in \mathscr{C}_+$ and that $v(0) \neq 0$. Then, $v(0) \in U(\mathscr{C})$ and $\phi(v)(0) = \theta^{\infty}(v)(0) = \theta(v(0)) = v(0) \neq 0$ which would show that $\phi(v) \neq 0$. This proves injectivity.

Regarding surjectivity, fix a $u \in (\mathscr{L}_{U(\mathscr{C})})_+$. For each $t \geqslant 0$ choose inductively $v_t \in \sigma^{-t}\mathscr{C}_+$ such that

$$\begin{cases} v_0(0) = u(0), \\ v_t(t) = u(t) - \sum_{s=0}^{t-1} \theta(v_s(t)), \quad t \geqslant 1 \end{cases}$$

and define $v := \sum_{t=0}^{+\infty} v_t$. Then, $\theta^{\infty}(v) \in (\mathscr{L}_{U(\mathscr{C})})_+$ and for each $t \geqslant 0$ we have that

$$\begin{aligned} \theta^{\infty}(v)(t) = \theta(v(t)) &= \theta\left(\sum_{s=0}^{+\infty} v_s(t)\right) = \sum_{s=0}^{t} \theta(v_s(t)) \\ &= \theta(v_t(t)) + \sum_{s=0}^{t} \theta(v_s(t)) = u(t). \end{aligned}$$

Consider now the causal shift operator $\psi := \phi^{-1} : \mathscr{L}_{U(\mathscr{C})} \to \mathscr{C}$. It remains to show that ψ is rational. Observe first that the inverse θ^{∞} of ψ is a static shift operator. We can apply Proposition 4 and we can argue that the canonical state space $X(\psi)$ of ψ is isomorphic to the canonical state space $X(\mathscr{C})$ of $\mathscr{C}$. By Theorem 1 this implies that $X(\psi)$ is a finite Abelian group and so ψ must be rational. □

Remark 5. The above result is also useful to characterize essentially systematic group codes: it is sufficient to replace V with the group $\mathscr{C}_{|[0]}$. In particular, we have that $\mathscr{C}$ is essentially systematic if and only if $U(\mathscr{C})$ splits in $\mathscr{C}_{|[0]}$.

4.4. Relation between minimal and systematic group codes

In this section the class of minimal encoders and the class of systematic encoders will be compared. As mentioned above, the class of systematic group codes is included in the class of minimal group codes. Actually, these two classes coincide for group codes having a $\mathbb{Z}_n$-free module as the encoding group. This fact, which has already been shown in [8] using polynomial matrices techniques, can also be proved using the previous results, as the following corollary shows.

Corollary 5. *Let $\mathscr{C} \subseteq \mathscr{L}_V$ be a group code and assume that the encoding group $W(\mathscr{C})$ is a $\mathbb{Z}_n$-free module for some integer n. Then the following conditions are equivalent*:

1. *$\mathscr{C}$ is minimal.*
2. *$\mathscr{C}$ is essentially systematic.*
3. *$U(\mathscr{C})$ is $\mathbb{Z}_n$-free.*

Proof. (1⇒3) follows from condition 2 of Theorem 2. (3⇒2) Since $W(\mathscr{C})$ is a $\mathbb{Z}_n$-module, then we have that also $\mathscr{C}_{|[0]}$ is a $\mathbb{Z}_n$-module. By 3 this implies that $U(\mathscr{C})$ splits in $\mathscr{C}_{|[0]}$ and so, by Theorem 4 and Remark 5, this yields 2. Finally, (2⇒1) is trivial. □

The relation existing between minimal group codes and systematic group codes can be clarified further by the following corollary. To present this result we need to introduce a transformation which can be performed on a group code. Fix $N \in \mathbb{N}$ and consider the map

$$P^N : \mathscr{L}_V \to \mathscr{L}_{V^N}$$

defined by

$$P^N(v)(t) := v_{|[tN,tN+N-1]}.$$

This map acts by cutting the sequence in pieces of length N. If $\mathscr{C} \subseteq \mathscr{L}_V$ is a group code, we define

$$\mathscr{C}^N := P^N(\mathscr{C}) \subseteq \mathscr{L}_{V^N}.$$

It is easy to see that $\mathscr{C}^N$ is still a group code and it is called the *Nth power* of $\mathscr{C}$. Notice that

$$U(\mathscr{C}^N) = \mathscr{C}_{+|[0,N-1]},$$

while

$$X(\mathscr{C}^N) \simeq \frac{(\mathscr{C}^N)^+}{(\mathscr{C}^N)_+} \simeq \frac{\mathscr{C}^+}{\mathscr{C}_+} \simeq X(\mathscr{C}).$$

Corollary 6. *Let $\mathscr{C} \subseteq \mathscr{L}_V$ be a group code. The following conditions are equivalent*:

1. *$\mathscr{C}$ is minimal.*
2. *$\mathscr{C}^N$ is essentially systematic, where $N \in \mathbb{N}$ is such that $\mathscr{C}$ is $(N+1)$-complete.*

Proof. (1⇒2) Let $N \in \mathbb{N}$ be such that $\mathscr{C}$ is $(N+1)$-complete. It follows from Theorem 4, Remark 5, and by the way $\mathscr{C}^N$ has been defined, that $\mathscr{C}^N$ is essentially systematic if and only if $U(\mathscr{C}^N) = \mathscr{C}_{+|[0,N-1]}$ splits in $\mathscr{C}^N_{|[0]} = \mathscr{C}_{|[0,N-1]}$. To prove this last condition, it is sufficient to show, by Lemma 1, that

$$n(\mathscr{C}_{|[0,N-1]}) \cap \mathscr{C}_{+|[0,N-1]} \subseteq n(\mathscr{C}_{+|[0,N-1]}).$$

Let $x \in \mathscr{C}_{|[0,N-1]}$ be such that $nx \in \mathscr{C}_{+|[0,N-1]}$. Let $v \in \mathscr{C}^+$ be such that $v_{|[0,N-1]} = x$. Hence, $nv_{|[0,N-1]} = nx \in \mathscr{C}_{+|[0,N-1]}$ and, by the way N has been chosen, we have that $nv \in \mathscr{C}_+$. It then follows from condition 3 of Theorem 3 that there exists $\tilde{v} \in \mathscr{C}_+$ such that $nv = n\tilde{v}$. This yields $nx = n\tilde{v}_{|[0,N-1]} \in n(\mathscr{C}_{+|[0,N-1]})$.

(2⇒1) If $\mathscr{C}^N$ is essentially systematic, it is also minimal. It then follows from Theorem 3 that $(\mathscr{C}^N)_+ \subseteq (\mathscr{C}^N)^+$ splits. Notice now that the transformation P_N induces an isomorphism both between $\mathscr{C}^+$ and $\mathscr{C}^{N+}$ and between $\mathscr{C}_+$ and $\mathscr{C}^N_+$. Therefore also $\mathscr{C}_+ \subseteq \mathscr{C}^+$ splits and, again by Theorem 3, this implies that $\mathscr{C}$ is minimal. □

5. Some numerical examples

In this last section we will present some examples of group codes. In particular we will show that

1. there exists a group code $\mathscr{C}$ which admits a causal encoder with causal inverse, but which is not a minimal group code;
2. there exists a minimal group code $\mathscr{C}$ which is not essentially systematic.

In order to treat these examples we need an algorithmic test verifying whether a subgroup H of an Abelian group G splits in G. In the following examples the group codes are modules over $\mathbb{Z}_n$ and so we will need a test which, given two matrices $M \in \mathbb{Z}_n^{h\times m}$ and $N \in \mathbb{Z}_n^{h\times l}$, is able to test whether H splits in G, where

$$G := \operatorname{im} M := \{Mx \in \mathbb{Z}_n^h : x \in \mathbb{Z}_n^m\},$$
$$H := \operatorname{im} N := \{Nx \in \mathbb{Z}_n^h : x \in \mathbb{Z}_n^l\}.$$

We developed an algorithmic test implemented in MAPLE V (available on request from the authors) which allowed us to verify whether H splits in G, by using Lemma 1. This procedure consisted in four subprocedures, whose correctness for aim of conciseness is not explicitly proved:

1. Given $M \in \mathbb{Z}_n^{h\times m}$, find $K \in \mathbb{Z}_n^{m\times g}$ such that
$$\operatorname{im} K = \ker M = \{x \in \mathbb{Z}_n^m : Mx = 0\}. \tag{19}$$
This can be done as follow. Let $\overline{M} \in \mathbb{Z}^{h\times m}$ be any representative of M and compute the Smith normal form over the Euclidean domain $\mathbb{Z}$
$$\begin{bmatrix}\overline{M} & nI_h\end{bmatrix} = \overline{U}\begin{bmatrix}\overline{\Lambda} & 0\\ 0 & 0\end{bmatrix}\overline{V},$$
where I_h is the $h \times h$-identity matrix, $\overline{U}$, $\overline{V}$ are unimodular integer matrices and where $\overline{\Lambda} = \operatorname{diag}\{k_1, \ldots, k_r\}$ with k_i nonzero integers. It can be shown that the matrix
$$K := \begin{bmatrix}I_m & 0\end{bmatrix}\overline{V}^{-1}\begin{bmatrix}0\\ I_{m+h-r}\end{bmatrix} \mod n$$
satisfies (19).
2. Given $M \in \mathbb{Z}_n^{h\times m}$ and $N \in \mathbb{Z}_n^{h\times l}$, find $L \in \mathbb{Z}_n^{h\times g}$ such that
$$\operatorname{im} L = \operatorname{im} M \cap \operatorname{im} N. \tag{20}$$
This can be done as follow. Let $F_1 \in \mathbb{Z}_n^{h\times g_1}$, $F_2 \in \mathbb{Z}_n^{h\times g_2}$ be such that
$$\ker\begin{bmatrix}M & -N\end{bmatrix} = \operatorname{im}\begin{bmatrix}F_1\\ F_2\end{bmatrix}$$
which can be computed by the procedure above. It can be shown that the matrix
$$L := MF_1$$
satisfies (20).
3. Given $M \in \mathbb{Z}_n^{h\times m}$ and $N \in \mathbb{Z}_n^{h\times l}$, test whether
$$\operatorname{im} N \subseteq \operatorname{im} M. \tag{21}$$
This can be done as follow. Let $\overline{M} \in \mathbb{Z}^{h\times m}$, $\bar{N} \in \mathbb{Z}^{h\times l}$ be any representatives of M and N respectively. Compute the Smith normal form over the Euclidean domain $\mathbb{Z}$
$$\begin{bmatrix}\overline{M} & nI_h\end{bmatrix} = \overline{U}\begin{bmatrix}\overline{\Lambda} & 0\\ 0 & 0\end{bmatrix}\overline{V},$$
where $\overline{U}$, $\overline{V}$ are unimodular integer matrices and where $\bar{\Lambda} = \operatorname{diag}\{k_1, \ldots, k_r\}$ with k_i nonzero integers. It can be shown that (21) holds true if and only if
$$\overline{\Lambda}^{-1}\begin{bmatrix}I_r & 0\end{bmatrix}\overline{U}^{-1}\overline{N} \text{ is an integer matrix,}$$
$$\begin{bmatrix}0 & I_{h-r}\end{bmatrix}\overline{U}^{-1}\overline{N} = 0.$$

4. Finally, given two matrices $M \in \mathbb{Z}_n^{h\times m}$ and $N \in \mathbb{Z}_n^{h\times l}$, to test whether $\operatorname{im} N$ splits in $\operatorname{im} M$, according to Lemma 1, it is enough to verify, for every ν dividing n, whether

   $$\operatorname{im} \nu M \cap \operatorname{im} N \subseteq \operatorname{im} \nu N$$

   and this can be done by using the previous procedures.

We applied this algorithm to the codes proposed in [2]. We noticed that most of these codes are essentially systematic, some are not even minimal and there are few codes which are not essentially systematic but are minimal. In the following we treat in detail three examples.

Example 1. Consider the first code of Table IX in [2]. In this case $V = \mathbb{Z}_4^2$. From the granules we can argue that the matrix

$$M = \begin{bmatrix} 2 & 3 \\ 2 & 1+2D \end{bmatrix} \in \mathbb{Z}_4[D, D^{-1}]^{2\times 2}$$

generates this code, namely, using the right multiplication convention, we have that

$$\begin{aligned} \mathscr{C} &= \operatorname{im} M(\sigma, \sigma^{-1}) \\ &= \left\{ \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \in \mathscr{L}_V \,\middle|\, \begin{array}{l} v_1(t) = 2w_1(t) + 3w_2(t) \\ v_2(t) = 2w_1(t) + w_2(t) + 2w_2(t-1) \end{array} \quad \exists w_1, w_2 \in \mathscr{L}_{\mathbb{Z}_4} \right\}. \end{aligned}$$

It is easy to verify that the polynomial matrix

$$N = \begin{bmatrix} 3 \\ 1+2D \end{bmatrix} \in \mathbb{Z}_4[D, D^{-1}]^{2\times 1}$$

represents a systematic encoder for $\mathscr{C}$ and so the encoding group of $\mathscr{C}$ is $\mathbb{Z}_4$. The existence of a systematic encoder is confirmed by the fact that $U(\mathscr{C})$ splits in V. The same arguments can be used to prove that all the codes of Table IX in [2] are systematic.

Example 2. Consider the first code of Table X in [2]. In this case $V = \mathbb{Z}_4^3$. From the granules we can argue that the matrix

$$M = \begin{bmatrix} 0 & 2 & 1 \\ 2 & 0 & D \\ 2 & 2 & 1+D \end{bmatrix} \in \mathbb{Z}_4[D, D^{-1}]^{3\times 3}$$

generates this code, namely, using the right multiplication convention, we have that

$$\begin{aligned} \mathscr{C} &= \operatorname{im} M(\sigma, \sigma^{-1}) \\ &= \left\{ \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} \in \mathscr{L}_V \,\middle|\, \begin{array}{l} v_1(t) = 2w_2(t) + w_3(t) \\ v_2(t) = 2w_1(t) + w_3(t-1) \\ v_3(t) = 2w_1(t) + 2w_2(t) \\ \qquad\quad + w_3(t) + w_3(t-1) \end{array} \quad \exists w_1, w_2, w_3 \in \mathscr{L}_{\mathbb{Z}_4} \right\}. \end{aligned}$$

It is easy to verify that the polynomial matrix

$$N = \begin{bmatrix} 1 & 0 \\ D & 2 \\ 1+D & 2 \end{bmatrix} \in \mathbb{Z}_4[D, D^{-1}]^{3\times 2}$$

represents an encoder for $\mathscr{C}$ and so the encoding group of $\mathscr{C}$ is $\mathbb{Z}_4 \oplus 2\mathbb{Z}_4$. Since, as pointed out in the table, the input group of this code is $\mathbb{Z}_4 \oplus 2\mathbb{Z}_4$, by Theorem 2 this code admits a causal encoder with causal inverse. In fact $N(\sigma, \sigma^{-1})$ is causal and admits the causal inverse represented by the matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 3D & 1 & 0 \end{bmatrix} \in \mathbb{Z}_4[D, D^{-1}]^{2\times 3}.$$

Using the properties of the granules [11] and defining the matrices

$$M_0 := \begin{bmatrix} 0 & 2 & 1 \\ 2 & 0 & 0 \\ 2 & 2 & 1 \end{bmatrix}, \quad M_1 := \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix},$$

we have that

$$\mathscr{C}_{|[0]} = \operatorname{im}[M_1\ M_0] \quad U(\mathscr{C}) = \mathscr{C}_{+|[0]} = \operatorname{im} M_0.$$

Applying the algorithm it can be verified that $U(\mathscr{C})$ does not split in $\mathscr{C}_{|[0]}$ and so $\mathscr{C}$ is neither systematic nor essentially systematic. It is not difficult to verify that

$$\mathscr{C} = \ker \begin{bmatrix} 1 & 1 & 3 \\ 2\sigma^{-1} & 2 & 0 \end{bmatrix} = \left\{ \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} \in \mathscr{L}_V \,\middle|\, \begin{matrix} v_1(t) + v_2(t) + 3v_3(t) = 0 \\ 2v_1(t-1) + 2v_2(t) = 0 \end{matrix} \right\}$$

which shows that $\mathscr{C}$ is 2-complete. By Corollary 3 we can argue that the group code $\mathscr{C}$ is not minimal.

Example 3. Consider the seventh code of Table X in [2]. Also in this case $V = \mathbb{Z}_4^3$. From the granules we can argue that the matrix

$$M = \begin{bmatrix} 2D & 2+D & 2 \\ 2D & D & 2+2D \\ 2 & 3+2D & 2+2D \end{bmatrix} \in \mathbb{Z}_4[D, D^{-1}]^{3\times 3}$$

generates this code, namely, using the right multiplication convention, we have that

$$\mathscr{C} = \operatorname{im} M(\sigma, \sigma^{-1}).$$

It can be verified that the polynomial matrix

$$N = \begin{bmatrix} 2+D & 2 \\ D & 2+2D \\ 3+2D & 2+2D \end{bmatrix} \in \mathbb{Z}_4[D, D^{-1}]^{3\times 2}$$

represents an encoder for $\mathscr{C}$ and so the encoding group of $\mathscr{C}$ is $\mathbb{Z}_4 \oplus 2\mathbb{Z}_4$. Since, as pointed out in the table, the input group of this code is $\mathbb{Z}_4 \oplus 2\mathbb{Z}_4$, by Theorem 2 this

code admits a causal encoder with causal inverse. In fact $N(\sigma, \sigma^{-1})$ is causal and admits the causal inverse represented by the matrix

$$\begin{bmatrix} 3+3D & 3+3D & 2+D \\ 3+2D & 3+2D & 3+2D \end{bmatrix} \in \mathbb{Z}_4[D, D^{-1}]^{2\times 3}.$$

Using the same reasonings used in the previous example and defining the matrices

$$M_0 := \begin{bmatrix} 0 & 2 & 2 \\ 0 & 0 & 2 \\ 2 & 3 & 2 \end{bmatrix} \quad M_1 := \begin{bmatrix} 2 & 1 & 0 \\ 2 & 1 & 2 \\ 0 & 2 & 2 \end{bmatrix},$$

we have that

$$\mathscr{C}_{|[0]} = \operatorname{im}[M_1\ M_0] \quad U(\mathscr{C}) = \mathscr{C}_{+|[0]} = \operatorname{im} M_0.$$

Applying the algorithm it can be verified that $U(\mathscr{C})$ does not split in $\mathscr{C}_{|[0]}$ and so $\mathscr{C}$ is neither systematic nor essentially systematic. It is not difficult to verify that

$$\mathscr{C} = \ker \begin{bmatrix} 1+3\sigma^{-2} & 2+3\sigma^{-2} & 3+3\sigma^{-1}+3\sigma^{-2} \\ 2 & 2 & 2 \end{bmatrix}$$

which shows that $\mathscr{C}$ is 3-complete. By Corollary 6 the group code $\mathscr{C}$ is minimal if and only if $\mathscr{C}^2$ (the 2nd power of $\mathscr{C}$) is essentially systematic and this happens if and only if

$$\mathscr{C}_{+|[0,1]} = \operatorname{im} \begin{bmatrix} M_0 & 0 \\ M_1 & M_0 \end{bmatrix}$$

splits in

$$\mathscr{C}_{|[0,1]} = \operatorname{im} \begin{bmatrix} M_1 & M_0 & 0 \\ 0 & M_1 & M_0 \end{bmatrix}.$$

Applying the algorithm it can be verified this occurs and so we can argue that $\mathscr{C}$ is minimal.

6. Conclusions

In this paper some characterizations of systematic and minimal convolutional codes over finite Abelian groups have been proposed. These characterizations yield effective algorithmic tests of these properties. We applied these tests to the codes proposed in [2] and we verified that all the possible situations actually occur. This shows that, as we could expect, in some cases the best codes are lost if we restrict to systematic and minimal convolutional codes. On the other hand, we point out that the same thing occurs when we restrict from general to linear codes. It would be important to quantify how much we loose with these restrictions and how much we gain in the simplification of the code synthesis. This is in fact the subject of our

present investigation in the specific field of the construction of parallel concatenated turbo TCM codes.

Another interesting topic to be investigated is the possibility of extending the theory presented in this paper to more general codes, such as codes over nonabelian groups, or codes over sequence spaces with semidirect group structures.

References

[1] S. Benedetto, D. Divsalar, G. Montorsi, F. Pollara, Serial concatenation of interleaved codes: performance analysis, design, and iterative decoding, IEEE Trans. Information Theory IT-44 (1998) 909–926.
[2] S. Benedetto, R. Garello, M. Mondin, G. Montorsi, Geometrically uniform TCM codes over groups based on L × MPSK constellations, IEEE Trans. Information Theory IT-40 (1994) 137–152.
[3] S. Benedetto, R. Garello, M. Mondin, M.D. Trott, Rotational invariance of trellis codes—Part II: Group codes and decoders, IEEE Trans. Information Theory IT-42 (1996) 766–778.
[4] W. Brewer, J.W. Bunce, F.S. Van Vleck, Linear Systems over Commutative Rings, Dekker, New York, 1986.
[5] R. Brockett, A.S. Willsky, Finite group homomorphic sequential systems, IEEE Trans. Automatic Control AC-17 (1972) 483–490.
[6] R. deB. Johnston, Linear systems over various rings, PhD thesis, Massachusetts Institute of Technology, 1973.
[7] F. Fagnani, S. Zampieri, Convolutional codes over finitely generated Abelian groups: some basic results, in: B. Marcus, J. Rosenthal (Eds.), Codes, Systems, and Graphical Models, volume 123 of IMA Volumes in Mathematics and its Applications, Springer Verlag, Berlin, 2000, pp. 327–346.
[8] F. Fagnani, S. Zampieri, System theoretic properties of convolutional codes over rings, IEEE Trans. Information Theory IT-47 (2001) 2256–2274.
[9] G.D. Forney, Convolutional codes I: Algebraic structure, IEEE Trans. Information Theory IT-16 (1970) 720–738.
[10] G.D. Forney, Geometrically uniform codes, IEEE Trans. Information Theory IT-37 (1991) 1241–1260.
[11] G.D. Forney, M.D. Trott, The dynamics of group codes: state spaces, trellis diagrams and canonical encoders, IEEE Trans. Information Theory IT-39 (1993) 1491–1513.
[12] R. Garello, G. Montorsi, S. Benedetto, D. Divsalar, F. Pollara, Labelings and encoders with the uniform bit error property with applications to serially concatenated trellis codes, IEEE Trans. Information Theory IT-48 (2002) 123–136.
[13] T.W. Hungerford, Algebra, Springer-Verlag, New York, 1974.
[14] R. Johannesson, Z. Wan, A linear algebra approach to minimal convolutional encoders, IEEE Trans. Information Theory IT-39 (1993) 1219–1233.
[15] R. Johannesson, Z. Wan, E. Wittenmark, Some structural properties of convolutional codes over rings, IEEE Trans. Information Theory IT-44 (1998) 839–845.
[16] R.E. Kalman, P.L. Falb, M.A. Arbib, Topics in Mathematical System Theory, McGraw-Hill, New York, 1969.
[17] H.A. Loeliger, T. Mittelholzer, Convolutional codes over groups, IEEE Trans. Information Theory IT-42 (1996) 1660–1686.
[18] J.L. Massey, T. Mittelholzer, Convolutional codes over rings, in: Proceedings of the Joint Swedish–Soviet International Workshop on Information Theory, Gotland, Sweeden, 1989, pp. 14–18.
[19] J.L. Massey, T. Mittelholzer, Systematicity and rotational invariance of convolutional codes over rings, in: Proceedings of the International Workshop on Algebra and Combinatorial Coding Theory, Leningrad, 1990, pp. 154–158.

[20] T. Mittelholzer, Minimal encoders for convolutional codes over rings, Communication Theory and Applications: Systems, Signal Processing and Error Control Coding, HW Comm. Ltd, 1993, pp. 30–36.
[21] E.D. Sontag, Linear systems over commutative rings: a survey, Ricerche di Automatica 7 (1976) 1–34.
[22] G. Ungerbock, Channel coding with multilevel phase signals, IEEE Trans. Information Theory IT-25 (1982) 55–67.
[23] J.C. Willems, Models for dynamics, Dynamics Reported 2 (1988) 171–269.